UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/961,293	09/25/2001	Shigeichiro Yamasaki	1504.1006	6803

21171 7590 03/24/2005

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/961,293	YAMASAKI ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 September 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 September 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *9-25-01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Remarks

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 – 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sims, "Media Content Protection Utilizing Public Key Cryptography", U.S. Patent 6,550,011 B1.

Regarding claim 1, Sims discloses a media content protection system designed to securely distribute and use content. He presents a cryptographic key management scheme for both authentication and encryption in a system for securely transferring content from content providers to content users (Sims, figs. 2A, 2B, 3 and 4). The system of Sims includes a data processing apparatus of a user for receiving a content supplied from a content transmitter (Sims, fig. 1, elem. 101). The data processing apparatus of the user is provided with a tamper-resistant device storing data inaccessible from outside (Sims, col. 11, lines 5-23). A content transmitter provides a

cipher to the content user, who in turn decodes the cipher (Sims, fig. 2A, elems. 200, 201, 202). Sims discloses a communications network connecting the system elements for mutual data communication (Sims, fig. 1, elem. 135).

While Sims makes mention of third party certification authorities (Sims, col. 5, lines 39-59), his disclosed key management scheme is handled largely by the content provider. The content provider of Sims, creates and provisions content, as well as encrypts and delivers content encryption keys. In addition, Sims discloses that the content provider could act as its own certification authority for public key cryptography authentication (Sims, col. 21, lines 48-51). Thus, Sims discloses the claimed apparatus and functionality of both a content transmitter and a trusted third party data processing apparatus combined into one, a content provider. Sims does not disclose a *data processing apparatus of a third party*.

As mentioned, the single content provider of Sims performs two system functions, whereas the applicant claims two system elements - a content transmitter for secure content creation and provision and a third party apparatus for enabling a secure key management scheme. The applicant logically separates the functionality of the content provider of Sims into a content transmitter and a third party apparatus. However, it would have been obvious to one of ordinary skill in the art, based upon legal precedent, to make separable the single content provider of Sims into the two claimed elements of the applicant, because the distinguishable division of labor would advantageously allow one system element to focus on content creation and provision

and the other system element to focus on enabling a secure key management scheme (In re Dulberg, 289 F.2d 522, 523, 129 USPQ 348, 349 (CCPA 1961)).

Therefore, the modification of Sims discloses a data processing apparatus of a third party trusted by both the content transmitter and the user (Sims, fig. 2A, elems. 200, 201), as well as wherein the data processing apparatus of the third party transmits first data to the data processing apparatus of the user, the first data relating to an encryption key that decodes a cipher generated by the content transmitter, the encryption key being obtained only within the tamper-resistant device (Sims, fig. 2A, elem. 201).

Regarding claim 2, it is essentially the same as claim 1, with the additional limitation:

wherein the data processing apparatus of the content transmitter supplies a cipher to the data processing apparatus of the user (Sims, fig. 2B);

Regarding claim 3, the modification of Sims discloses:

wherein the data processing apparatus of the third party stores a public key and a secret key, the public key being transmitted to the data processing apparatus of the content transmitter as required by the data processing apparatus of the content transmitter (Sims, col. 5, lines 35-59);

wherein the data processing apparatus of the content transmitter encodes the encryption key by using the public key from the data processing apparatus of the third

party, the encoded encryption key being transmitted to the data processing apparatus of the user (Sims, col. 5, lines 53-59; fig. 2A, elem. 201);

wherein the data processing apparatus of the user causes the tamper-resistant device to generate second data based on the encoded encryption key from the data processing apparatus of the content transmitter, the second data being transmitted to the data processing apparatus of the third party (Sims, col. 16, lines 18-29). The tamper-resistant device "generates" second data based upon the encoded encryption key by generating a random number and sending it to an originating device, where it is combined with the encoded encryption key. Since the "originating device" is part of the disclosed secure key management scheme of Sims, the originating device is part of the obvious third party apparatus disclosed in the modification of Sims.

and wherein the data processing apparatus of the third party generates the first data based on the secret key and the second data supplied from the data processing apparatus of the user (Sims, col. 16, lines 44-52).

Regarding claim 4, the modification of Sims discloses:

an additional third party, wherein the tamper-resistant device divides the second data into pieces one of which is received by a relevant one of the third parties (Sims, fig. 1; col. 16, lines 44-60). As disclosed, the tamper-resistant device divides the second data (content key + random number) and stores the content key (separated from the

second data) in an appropriate area, such as an additional third party (Sims, fig.1, elem. 112).

Regarding claim 5, the modification of Sims discloses:

wherein the tamper-resistant device allows mixing of a random number component in generating the second data based on the encoded encryption key, while also allowing removal of the random number component from the first data in decoding the cipher by using the first data (Sims, col. 16, lines 18-29).

Regarding claim 6, the modification of Sims discloses:

wherein the tamper-resistant device stores information on the public key in a form of a digital certificate by an authentication agency, the tamper-resistant device being supplied to the user after the user is identified by the authentication agency (Sims, col. 14, lines 49-59; col. 15, lines 22-26; col. 21, lines 16-20). Sims discloses that digital certificates are stored on the tamper-resistant devices and that the identity of a user of a device is tied to the device itself, and therefore, the user is identified by the authentication agency.

and wherein the data processing apparatus of the third party confirms the identification of the user based on the public key information supplied in the form of the digital certificate from the data processing apparatus of the user (Sims, col. 12, lines 23-30).

Regarding claim 7, the modification of Sims discloses the tamper-resistant device comprising:

a memory storing data inaccessible from outside (Sims, fig. 1, elems. 112, 113, 117, 116);

a key obtainer that restores the decoding key based on the key data supplied from the data processing apparatus of the third party (Sims, fig. 1, elems. 112, 113, 117, 116);;

and a decoder that decodes the encrypted content by using the decoding key restored by the key obtainer (Sims, fig. 1, elems. 112, 113, 117, 116);

Regarding claim 8, the modification of Sims discloses the server comprising:

a data generator that generates first data relating to a key to decode the encrypted content from the data processing apparatus of the content transmitter, the decoding key being generated only within the tamper-resistant device (Sims, col. 16, lines 18-43). The originating device, part of the third party apparatus as explained regarding claim 3, generates the first data.

and a data transmitter that sends the first data to the data processing apparatus of the user via the communications network (Sims, col. 16, lines 46-52).

Regarding claim 9, it is a computer program version of the server claim 8, and is rejected by the same rationality.

Regarding claim 10, the modification of Sims discloses a content distribution process comprising the steps of:

causing the data processing apparatus of the user to issue an instruction to the data processing apparatus of the third party for carrying out a procedure to make a payment for the content (Sims, col. 7, lines 21-27);

causing the data processing apparatus of the third party to send first data to the data processing apparatus of the user when the payment for the content is made from an account of the user to an account of the third party, the first data serving to provides a key that decodes the encrypted content, the decoding key being available only within the data processing apparatus of the user (Sims, col. 9, lines 33-40);

and causing the data processing apparatus of the user to decode the encrypted content using the first data supplied from the data processing apparatus of the third party (Sims, col. 9, lines 40-42).

Regarding claims 11 – 13, they recite the same limitations found in claims 2, 3, and 5, and are rejected for the same reasons.

Regarding claim 14, the modification of Sims discloses:

wherein the tamper- resistant device generates the second data and decodes the encrypted content (Sims, col. 16, lines 18-29; fig. 2A, elem. 202).

Regarding claim 15, the modification of Sims discloses:

wherein the data processing apparatus of the third party carries out the payment procedure from the account of the third party to the account of the content transmitter when the data processing apparatus of the third party receives content confirmation notice from the data processing apparatus of the user (Sims, col. 7, lines 21-27; col. 9, lines 33-40). Sims discloses before payment for content, the user transmits to the third party his request for that particular content, thus providing a content confirmation notice.

Conclusion

The following prior art made of record and not relied upon is considered pertinent to the applicant's disclosure:

a. Graunke et al., "Method for Securely Distributing a Conditional Use Private Key to a Trusted Entity on a Remote System", U.S. Patent 5,991,399.

b. Spies et al., "System and Method For Secure Purchase and Delivery of Video Content Programs", U.S. Patent 6,055,314.

c. Wang et al., "System and Method for Transferring the Right to Decode Messages in a Symmetric Encoding Scheme", U.S. Patent 6,859,533 B1.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
(571) 272-7965
March 17, 2005

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER